

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-073415

(43)Date of publication of application : 18.03.1997

(51)Int.Cl. G06F 12/14
G06K 17/00
G09C 1/00
H04L 9/10

(21)Application number : 08-178188

(71)Applicant : THOMSON CONSUMER ELECTRON INC

(22)Date of filing : 08.07.1996

(72)Inventor : ROHATGI PANKAJ

(30)Priority

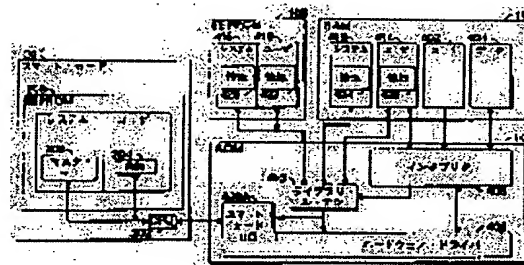
Priority number : 95 499170 Priority date : 07.07.1995 Priority country : US

(54) METHOD FOR SAFELY STORING SENSITIVE INFORMATION IN STORAGE MEDIUM WITH RELATIVELY LOW SAFETY DEGREE AND DEVICE THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide method and device safely storing sensitive information in a computer system including a storage medium with relatively high safety degree and a storage medium with relatively low safety degree.

SOLUTION: Sensitive information is ciphered by using a cryptographic key 302. Next, the ciphered sensitive information is stored in storage media 108 and 104 with relatively low safety degree and the cryptographic key 302 is stored in a storage medium 208 with relatively high safety degree. By this device, sensitive information is safely stored in the computer system including the storage medium 208 with relatively high safety degree in which the cryptographic key 302 is stored and storage media 108 and 104 with relatively low safety degree. A ciphering device 202 ciphers sensitive information by using the cryptographic key 302 and stores the ciphered sensitive information in storage media 108 and 104 with relatively low safety degree.

**LEGAL STATUS**

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

BEST AVAILABLE COPY

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-73415

(43)公開日 平成9年(1997)3月18日

(51)Int.Cl. ⁹	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0		G 0 6 F 12/14	3 2 0 B
G 0 6 K 17/00			G 0 6 K 17/00	S
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 A
H 0 4 L 9/10			H 0 4 L 9/00	6 2 1 A

審査請求 未請求 請求項の数20 O L (全 14 頁)

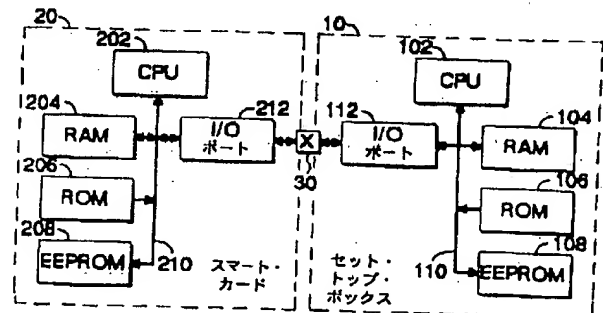
(21)出願番号	特願平8-178188	(71)出願人	391000818 トムソン コンシューマ エレクトロニク ス インコーポレイテッド THOMSON CONSUMER EL ECTRONICS, INCORPORA TED アメリカ合衆国 インディアナ州 46290 -1024 インディアナポリス ノース・メ リディアン・ストリート 10330
(22)出願日	平成8年(1996)7月8日	(72)発明者	パンカジャ ロハトギ アメリカ合衆国 94086 カリフォルニア 州 サニーヴェイル ヴィンセント ドラ イブ 1256 アパートメント エイチ
(31)優先権主張番号	08/499170	(74)代理人	弁理士 谷 義一 (外1名)
(32)優先日	1995年7月7日		
(33)優先権主張国	米国 (US)		

(54)【発明の名称】 センシティブ情報を相対的に安全度の低い記憶媒体に安全にストアする方法および装置

(57)【要約】

【課題】 相対的に安全度の高い記憶媒体と相対的に安全度の低い記憶媒体を含んでいるコンピュータ・システムにおいてセンシティブ情報を安全にストアする方法および装置が開示されている。

【解決手段】 センシティブ情報は暗号キーを使用して暗号化される。次に、暗号化されたセンシティブ情報は相対的に安全度の低い記憶媒体にストアされ、暗号キーは相対的に安全度の高い記憶媒体にストアされる。また、この装置によれば、暗号キー (302) がストアされる相対的に安全度の高い記憶媒体 (208) と、相対的に安全度の低い記憶媒体 (108, 104) とを含んでいるコンピュータ・システムにおいて、センシティブ情報を安全にストアする。暗号化器 (202) は暗号キーを使用してセンシティブ情報を暗号化し、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体にストアする。



【特許請求の範囲】

【請求項 1】 相対的に安全度の高い記憶媒体と相対的に安全度の低い記憶媒体とを備えたコンピュータ・システムにおいて、センシティブ情報を相対的に安全度の低い記憶媒体にストアする方法であって、暗号キーを使用してセンシティブ情報を暗号化するステップと、

暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体にストアするステップと、暗号キーを相対的に安全度の高い記憶媒体にストアするステップとを含むことを特徴とする方法。

【請求項 2】 請求項 1 に記載の方法において、相対的に安全度の高い記憶媒体はプロセッサとメモリを含んでおり、さらに、暗号キーをストアするステップは、暗号キーをプロセッサに与えるステップと、暗号キーをプロセッサからメモリに転送するステップとを含む、

センシティブ情報を暗号化するステップは、センシティブ情報をプロセッサに与えるステップと、プロセッサ内のセンシティブ情報を、以前にメモリにストアされた暗号キーを使用して暗号化するステップと、相対的に安全度の低い記憶媒体にストアするために、暗号化されたセンシティブ情報をプロセッサから返却するステップとを含むことを特徴とする方法。

【請求項 3】 請求項 1 に記載の方法において、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体から取り出すステップと、取り出された暗号化されたセンシティブ情報を暗号キーを使用して暗号解読するステップとをさらに含むことを特徴とする方法。

【請求項 4】 請求項 1 に記載の方法において、相対的に安全度の高い記憶媒体はプロセッサとメモリを含んでおり、さらに、センシティブ情報を暗号解読するステップは、取り出された暗号化されたセンシティブ情報をプロセッサに与えるステップと、プロセッサ内の取り出されたセンシティブ情報を暗号キーを使用して暗号解読するステップと、暗号解読されたセンシティブ情報をプロセッサから返却するステップとを含むことを特徴とする方法。

【請求項 5】 請求項 3 に記載の方法において、センシティブ情報を暗号化するステップは暗号化されたセンシティブ情報全体にわたって暗号チェックサムを計算するステップを含み、暗号化されたセンシティブ情報をストアするステップは暗号チェックサムをストアするステップを含み、暗号解読するステップは、以前にストアされた暗号チェックサムを取り出すステップと、

ストアされた暗号化されたセンシティブ情報全体にわたって暗号チェックサムを計算するステップと、以前にストアされた暗号チェックサムを、新たに計算された暗号チェックサムと比較するステップと、以前にストアされた暗号チェックサムが新たに計算された暗号チェックサムと不一致であれば、エラーを返却するステップとを含むことを特徴とする方法。

【請求項 6】 請求項 3 に記載の方法において、取り出すステップの前に、取出し権限をユーザに要求するステップと、取出し権限をユーザから受け取ったときだけ、取出しステップと暗号解読ステップを実行するステップとをさらに含むことを特徴とする方法。

【請求項 7】 請求項 6 に記載の方法において、取出し権限を要求するステップは、識別ストリング (string) をユーザに要求するステップと、ユーザから識別ストリングを受け取るステップと、受け取った識別ストリングを、あらかじめ決めた識別ストリングと比較するステップと、受け取った識別ストリングがあらかじめ決めた識別ストリングと一致していれば、取出し権限がユーザから受け取られたと判定するステップとを含むことを特徴とする方法。

【請求項 8】 請求項 7 に記載の方法において、暗号キーをストアするステップはあらかじめ決めた識別ストリングを相対的に安全度の高い記憶媒体にストアするステップを含むことを特徴とする方法。

【請求項 9】 請求項 7 に記載の方法において、暗号キーをストアするステップは、あらかじめ決めた識別ストリングを暗号キーを使用して暗号化するステップと、暗号化されたあらかじめ決めた識別ストリングを相対的に安全度の低い記憶媒体にストアするステップとを含み、比較するステップは、暗号化されたあらかじめ決めた識別ストリングを相対的に安全度の低い記憶媒体から取り出すステップと、暗号化されたあらかじめ決めた識別ストリングを暗号ストリングを使用して暗号解読するステップと、ユーザからの識別ストリングを、暗号解読されたあらかじめ決めた識別ストリングと比較するステップとを含むことを特徴とする方法。

【請求項 10】 請求項 9 に記載の方法において、あらかじめ決めた識別ストリングを暗号化するステップはあらかじめ決めた識別ストリング全体にわたって暗号チェックサムを計算するステップを含み、暗号化されたあらかじめ決めた識別ストリングをストアするステップは暗号チェックサムも相対的に安全度の低い記憶媒体にストアするステップを含み、

暗号化されたあらかじめ決めた識別ストリングを取り出すステップは以前にストアされた暗号チェックサムも取り出すステップを含み、
暗号化されたあらかじめ決めた識別ストリングを暗号解読するステップは、
あらかじめ決めた識別ストリング全体にわたって暗号チェックサムを計算するステップと、
計算された暗号チェックサムを、取り出された暗号チェックサムと比較するステップと、
計算された暗号チェックサムが取り出された暗号チェックサムと一致しているときだけ、受け取った識別ストリングを、暗号解読したあらかじめ決めた識別ストリングと比較するステップを実行するステップとを含むことを特徴とする方法。

【請求項 11】 請求項 1 に記載の方法において、
センシティブ情報を暗号化するステップは暗号化されたセンシティブ情報全体にわたって暗号チェックサムを計算するステップを含み、
暗号化されたセンシティブ情報をストアするステップは暗号チェックサムを暗号化されたセンシティブ情報と一緒にストアするステップを含むことを特徴とする方法。

【請求項 12】 インタラクティブ・テレビジョン・システムにおいてセンシティブ情報を安全にストアするプロセッサ装置であって、
暗号キーをストアするための相対的に安全度の高い記憶媒体と、
相対的に安全度の低い記憶媒体と、
相対的に安全度の低い記憶媒体に結合されていて、暗号キーに応答してセンシティブ情報を暗号化し、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体にストアする暗号化器とを備えていることを特徴とする装置。

【請求項 13】 請求項 12 に記載の装置において、
暗号解読器をさらに含み、該暗号解読器は相対的に安全度の低い記憶媒体に結合されていて、暗号キーに応答して暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体から取り出し、暗号化されたセンシティブ情報を暗号解読することを特徴とする装置。

【請求項 14】 請求項 13 に記載の装置において、
暗号解読器は取出し権限をユーザに要求し、取出し権限をユーザから受け取ったときだけ、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体から取り出し、暗号化されたセンシティブ情報を暗号解読する回路を含むことを特徴とする装置。

【請求項 15】 請求項 14 に記載の装置において、
取出し権限を要求する回路は、
識別ストリングをユーザに要求する回路と、
受け取った識別ストリングをあらかじめ決めた識別ストリングと比較し、受け取った識別ストリングがあらかじめ決めた識別ストリングと一致していれば、取出し権限

が受け取られたと判定する回路とを含むことを特徴とする装置。

【請求項 16】 請求項 15 に記載の装置において、
あらかじめ決めた識別ストリングは暗号化された形態で相対的に安全度の低い記憶媒体にストアされ、暗号解読器は、さらに、
暗号化されたあらかじめ決めた識別ストリングを相対的に安全度の低い記憶媒体から受け取る回路と、
前記受け取った暗号化されたあらかじめ決めた識別ストリングを暗号解読する回路とを含むことを特徴とする装置。

【請求項 17】 請求項 12 に記載の装置において、
相対的に安全度の高い記憶媒体は、
マイクロプロセッサと、
システム・バスを介してマイクロプロセッサに結合されていて、暗号キーをストアするためのメモリとを含んでおり、
暗号化器と暗号解読器はマイクロプロセッサに含まれていることを特徴とする装置。

【請求項 18】 請求項 17 に記載の装置において、
相対的に安全度の低い記憶媒体は、
別のマイクロプロセッサと、
システム・バスを介してマイクロプロセッサに結合されていて、暗号化されたセンシティブ情報をストアするための読み書きメモリとを含んでいることを特徴とする装置。

【請求項 19】 請求項 18 に記載の装置において、
相対的に安全度の高い記憶媒体はさらに入出力ポートを含み、該入出力ポートは相対的に安定度の高い記憶媒体側のシステム・バスを介して、相対的に安定度の高い記憶媒体側のマイクロプロセッサとメモリに結合されており、
相対的に安定度の低い記憶媒体はさらに入出力ポートを含み、該入出力ポートは相対的に安定度の低い記憶媒体側のシステム・バスを介して、相対的に安定度の低い記憶媒体側の別のマイクロプロセッサとメモリに結合されており、
相対的に安定度の高い記憶媒体側の入出力ポートは相対的に安定度の低い記憶媒体側の入出力ポートに結合されていることを特徴とする装置。

【請求項 20】 請求項 12 に記載の装置において、
さらに、前記暗号化されたセンシティブ情報全体にわたってチェックサムを生成し、当該チェックサムを、ストアされた前記暗号化されたセンシティブ情報に付加する回路と、
ストアされた前記暗号化されたセンシティブ情報全体にわたって別のチェックサムを生成し、当該別のチェックサムを、前記ストアされた暗号化されたセンシティブ情報に付加された前記チェックサムと比較する回路と、
前記チェックサムと前記別のチェックサムが同一である

10

20

30

40

50

ことを条件として、前記ストアされた暗号化されたセンシティブ情報を暗号解読する暗号解読器とを含むことを特徴とする装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、センシティブ情報を相対的に安全度の低い記憶媒体にストアする方法および装置に関する。

【0002】なお、本明細書の記述は本件出願の優先権の基礎たる米国特許出願第08/499,170号(1995年7月7日出願)の明細書の記載に基づくものであって、当該米国特許出願の番号を参照することによって当該米国特許出願の明細書の記載内容が本明細書の一部を構成するものとする。

【0003】

【従来の技術】センシティブ情報(例えば、クレジットカード番号または暗号キー)をコンピュータ・システムにストアしておく必要がしばしば起こっている。しかし、かかるセンシティブ情報のストアの仕方が安全でないと、その情報が変更されたり、盗まれたりする可能性がある。コンピュータ・システムへのアクセスを信用のある人だけに制限し、信用のあるプログラムだけをコンピュータ・システムで実行することは、この問題を解決する1つの方法である。しかし、この解決方法は常に実用的であるとは限らない。第三者による使用を目的としていても、第三者によるアクセスを認めなければ、無用になってしまうコンピュータ・システムが存在するからである。例えば、インタラクティブ(対話型)テレビジョン・システムのようなマルチメディア・システムでは、ユーザのデコーダはユーザのセンシティブ情報をストアしているが、見知らぬ第三者が書いたプログラムを実行するために、やむを得ずそのデコーダが利用されることがある。

【0004】インタラクティブ・テレビジョン・アプリケーションはビデオ(映像)部分、オーディオ(音声)部分およびコンピュータ・プログラム部分からなっている。このインタラクティブ・テレビジョン・アプリケーションは、中央のブロードキャスト・ロケーションから遠隔地の視聴者(viewer)ロケーションへコンポジット信号でブロードキャスト(同報通信)されている。各視聴者のロケーションにはレシーバ/デコーダが置かれており、これらはインタラクティブ・テレビジョン・アプリケーションのコンポジット信号を検出・出力し、ビデオ部分、オーディオ部分およびコンピュータ・プログラム部分を分離し、テレビジョン・レシーバが必要とするビデオ信号とオーディオ信号を生成し、コンピュータ・プログラムを実行して視聴者と対話している。各デコーダは電話インタフェースも備えているので、コンピュータ・プログラムの制御の下で(およびユーザの許可を得て)データ・コール(起呼)を行って、リモート・ロケ

ーションとの間で情報(実行すべきコンピュータ・プログラム・コードを含む)を送受信することを可能にしている。

【0005】

【発明が解決しようとする課題】ここで検討しようとしている1つのインタラクティブ・アプリケーションはショッピング・アプリケーションであり、このアプリケーションでは、以前にデコーダに入力されていた視聴者のクレジットカード番号は、視聴者がオーダーを出したとき、安全な方法で(ユーザの許可を得て)ショッピング・プログラム提供者へ送られるようにしている。そのために、視聴者のクレジットカード番号はデコーダにストアしておく必要がある。しかし、コンピュータ・プログラムはブロードキャストまたは電話リンクを通してロード可能であるので、そのコンピュータ・プログラムが視聴者のクレジットカード番号や他のセンシティブ情報を盗んでそれを、例えば、電話リンクを通して第三者へ中継しようとすることも起こり得る。

【0006】センシティブ情報を安全に維持するための1つの方法では、コンピュータ・システムの公用部分と、センシティブ情報がストアされる部分との間の障壁となるために、ハードウェアをコンピュータ・システムに接続することが要件になっている。しかし、ハードウェアによる解決は高価である。これは、コンシューマ・プロダクトであるインタラクティブ・テレビジョン・システムでは、コストに非常に敏感であるために特に問題である。そのために、この種のシステムで利用可能にされる安全保護ハードウェア量は、最小限の情報を収容して、保護するような設計になっている。しかし、盗難から保護する必要のあるセンシティブ情報は大量化する潜在性をもっている。望ましいことは、比較的に大量のセンシティブ情報を変更または盗難から保護し、しかも、高価な安全保護ハードウェアを大量に使用しないで済むようにすることである。

【0007】

【課題を解決するための手段】本発明の原理によれば、相対的に安全度の高い記憶媒体と相対的に安全度の低い記憶媒体を備えたコンピュータ・システムにおいて、センシティブ情報を安全にストアする方法は次のようなステップからなっている。センシティブ情報は暗号キーを使用して暗号化される。暗号化されたセンシティブ情報は相対的に安全度の低い記憶媒体にストアされ、暗号キーは相対的に安全度の高い記憶媒体にストアされる。

【0008】コンピュータ・システムにおいてセンシティブ情報を安全にストアする装置は暗号キーがストアされる相対的に安全度の高い記憶媒体と、相対的に安全度の低い記憶媒体とを含んでいる。暗号化器(encrypter)は暗号キーを使用してセンシティブ情報を暗号化し、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体にストアする。

【0009】請求項1にかかる発明は、相対的に安全度の高い記憶媒体と相対的に安全度の低い記憶媒体とを備えたコンピュータ・システムにおいて、センシティブ情報を相対的に安全度の低い記憶媒体にストアする方法であって、暗号キーを使用してセンシティブ情報を暗号化するステップと、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体にストアするステップと、暗号キーを相対的に安全度の高い記憶媒体にストアするステップとを含むことを特徴とする。

【0010】また、請求項2にかかる発明は、請求項1に記載の方法において、相対的に安全度の高い記憶媒体はプロセッサとメモリを含んでおり、さらに、暗号キーをストアするステップは、暗号キーをプロセッサに与えるステップと、暗号キーをプロセッサからメモリに転送するステップとを含み、センシティブ情報を暗号化するステップは、センシティブ情報をプロセッサに与えるステップと、プロセッサ内のセンシティブ情報を、以前にメモリにストアされた暗号キーを使用して暗号化するステップと、相対的に安全度の低い記憶媒体にストアするために、暗号化されたセンシティブ情報をプロセッサから返却するステップとを含むことを特徴とする。

【0011】さらに、請求項3にかかる発明は、請求項1に記載の方法において、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体から取り出すステップと、取り出された暗号化されたセンシティブ情報を暗号キーを使用して暗号解読するステップとをさらに含むことを特徴とする。

【0012】さらに、請求項4にかかる発明は、請求項1に記載の方法において、相対的に安全度の高い記憶媒体はプロセッサとメモリを含んでおり、さらに、センシティブ情報を暗号解読するステップは、取り出された暗号化されたセンシティブ情報をプロセッサに与えるステップと、プロセッサ内の取り出されたセンシティブ情報を暗号キーを使用して暗号解読するステップと、暗号解読されたセンシティブ情報をプロセッサから返却するステップとを含むことを特徴とする。

【0013】さらに、請求項5にかかる発明は、請求項3に記載の方法において、センシティブ情報を暗号化するステップは暗号化されたセンシティブ情報全体にわたって暗号チェックサムを計算するステップを含み、暗号化されたセンシティブ情報をストアするステップは暗号チェックサムをストアするステップを含み、暗号解読するステップは、以前にストアされた暗号チェックサムを取り出すステップと、ストアされた暗号化されたセンシティブ情報全体にわたって暗号チェックサムを計算するステップと、以前にストアされた暗号チェックサムを、新たに計算された暗号チェックサムと比較するステップと、以前にストアされた暗号チェックサムが新たに計算された暗号チェックサムと不一致であれば、エラーを返却するステップとを含むことを特徴とする。

【0014】さらに、請求項6にかかる発明は、請求項3に記載の方法において、取り出すステップの前に、取出し権限をユーザに要求するステップと、取出し権限をユーザから受け取ったときだけ、取出しステップと暗号解読ステップを実行するステップとをさらに含むことを特徴とする。

【0015】さらに、請求項7にかかる発明は、請求項6に記載の方法において、取出し権限を要求するステップは、識別ストリング(string)をユーザに要求するステップと、ユーザから識別ストリングを受け取るステップと、受け取った識別ストリングを、あらかじめ決めた識別ストリングと比較するステップと、受け取った識別ストリングがあらかじめ決めた識別ストリングと一致していれば、取出し権限がユーザから受け取られたと判定するステップとを含むことを特徴とする。

【0016】さらに、請求項8にかかる発明は、請求項7に記載の方法において、暗号キーをストアするステップはあらかじめ決めた識別ストリングを相対的に安全度の高い記憶媒体にストアするステップを含むことを特徴とする。

【0017】さらに、請求項9にかかる発明は、請求項7に記載の方法において、暗号キーをストアするステップは、あらかじめ決めた識別ストリングを暗号キーを使用して暗号化するステップと、暗号化されたあらかじめ決めた識別ストリングを相対的に安全度の低い記憶媒体にストアするステップとを含み、比較するステップは、暗号化されたあらかじめ決めた識別ストリングを相対的に安全度の低い記憶媒体から取り出すステップと、暗号化されたあらかじめ決めた識別ストリングを暗号ストリングを使用して暗号解読するステップと、ユーザからの識別ストリングを、暗号解読されたあらかじめ決めた識別ストリングと比較するステップとを含むことを特徴とする方法。

【0018】さらに、請求項10にかかる発明は、請求項9に記載の方法において、あらかじめ決めた識別ストリングを暗号化するステップはあらかじめ決めた識別ストリング全体にわたって暗号チェックサムを計算するステップを含み、暗号化されたあらかじめ決めた識別ストリングをストアするステップは暗号チェックサムも相対的に安全度の低い記憶媒体にストアするステップを含み、暗号化されたあらかじめ決めた識別ストリングを取り出すステップは以前にストアされた暗号チェックサムも取り出すステップを含み、暗号化されたあらかじめ決めた識別ストリングを暗号解読するステップは、あらかじめ決めた識別ストリング全体にわたって暗号チェックサムを計算するステップと、計算された暗号チェックサムを、取り出された暗号チェックサムと比較するステップと、計算された暗号チェックサムが取り出された暗号チェックサムと一致しているときだけ、受け取った識別ストリングを、暗号解読したあらかじめ決めた識別スト

リングと比較するステップを実行するステップとを含むことを特徴とする。

【0019】さらに、請求項11にかかる発明は、請求項1に記載の方法において、センシティブ情報を暗号化するステップは暗号化されたセンシティブ情報全体にわたって暗号チェックサムを計算するステップを含み、暗号化されたセンシティブ情報をストアするステップは暗号チェックサムを暗号化されたセンシティブ情報と一緒にストアするステップを含むことを特徴とする。

【0020】さらに、請求項12にかかる発明は、インタラクティブ・テレビジョン・システムにおいてセンシティブ情報を安全にストアするプロセッサ装置であって、暗号キーをストアするための相対的に安全度の高い記憶媒体(208)と、相対的に安全度の低い記憶媒体(108, 104)と、相対的に安全度の低い記憶媒体に結合されていて、暗号キー(302)に応答してセンシティブ情報を暗号化し、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体にストアする暗号化器(202)とを備えていることを特徴とする。

【0021】さらに、請求項13にかかる発明は、請求項12に記載の装置において、暗号解読器をさらに含み、該暗号解読器は相対的に安全度の低い記憶媒体に結合されていて、暗号キーに応答して暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体から取り出し、暗号化されたセンシティブ情報を暗号解読することを特徴とする。

【0022】さらに、請求項14にかかる発明は、請求項13に記載の装置において、暗号解読器は取出し権限をユーザに要求し、取出し権限をユーザから受け取ったときだけ、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体から取り出し、暗号化されたセンシティブ情報を暗号解読する回路を含むことを特徴とする。

【0023】さらに、請求項15にかかる発明は、請求項14に記載の装置において、取出し権限を要求する回路は、識別ストリングをユーザに要求する回路と、受け取った識別ストリングをあらかじめ決めた識別ストリングと比較し、受け取った識別ストリングがあらかじめ決めた識別ストリングと一致していれば、取出し権限が受け取られたと判定する回路とを含むことを特徴とする。

【0024】さらに、請求項16にかかる発明は、請求項15に記載の装置において、あらかじめ決めた識別ストリングは暗号化された形態で相対的に安全度の低い記憶媒体にストアされ、暗号解読器は、さらに、暗号化されたあらかじめ決めた識別ストリングを相対的に安全度の低い記憶媒体から受け取る回路と、前記受け取った暗号化されたあらかじめ決めた識別ストリングを暗号解読する回路とを含むことを特徴とする。

【0025】さらに、請求項17にかかる発明は、請求項12に記載の装置において、相対的に安全度の高い記

憶媒体は、マイクロプロセッサと、システム・バスを介してマイクロプロセッサに結合されていて、暗号キーをストアするためのメモリとを含んでおり、暗号化器と暗号解読器はマイクロプロセッサに含まれていることを特徴とする。

【0026】さらに、請求項18にかかる発明は、請求項17に記載の装置において、相対的に安全度の低い記憶媒体は、別のマイクロプロセッサと、システム・バスを介してマイクロプロセッサに結合されていて、暗号化されたセンシティブ情報をストアするための読み書きメモリとを含んでいることを特徴とする。

【0027】さらに、請求項19にかかる発明は、請求項18に記載の装置において、相対的に安全度の高い記憶媒体はさらに入出力ポートを含み、該入出力ポートは相対的に安定度の高い記憶媒体側のシステム・バスを介して、相対的に安定度の高い記憶媒体側のマイクロプロセッサとメモリに結合されており、相対的に安定度の低い記憶媒体はさらに入出力ポートを含み、該入出力ポートは相対的に安定度の低い記憶媒体側のシステム・バスを介して、相対的に安定度の低い記憶媒体側の別のマイクロプロセッサとメモリに結合されており、相対的に安定度の高い記憶媒体側の入出力ポートは相対的に安定度の低い記憶媒体側の入出力ポートに結合されていることを特徴とする。

【0028】さらに、請求項20にかかる発明は、請求項12に記載の装置において、さらに、前記暗号化されたセンシティブ情報全体にわたってチェックサムを生成し、当該チェックサムを、ストアされた前記暗号化されたセンシティブ情報に付加する回路と、ストアされた前記暗号化されたセンシティブ情報全体にわたって別のチェックサムを生成し、当該別のチェックサムを、前記ストアされた暗号化されたセンシティブ情報に付加された前記チェックサムと比較する回路と、前記チェックサムと前記別のチェックサムが同一であることを条件として、前記ストアされた暗号化されたセンシティブ情報を暗号解読する暗号解読器とを含むことを特徴とする。

【0029】

【発明の実施の形態】図1は、本発明を取り入れているインタラクティブ・テレビジョン・デコーダを示すブロック図である。図1に示すように、セット・トップ・ボックス(set topbox)10はスマート・カード20に結合されている。スマート・カード20は例えば、クレジットカードとほぼ同サイズの小型デバイスであり、これはセット・トップ・ボックス10内のコネクタ30に挿入される。セット・トップ・ボックス10はCPU102を内蔵しており、このCPUは、システム・バス110を介して公知のようにRAM104、ROM106、EEPROM108および入出力(I/O)ポート112に結合されている。セット・トップ・ボックス10は他の入出力ポート(図示せず)も備えており、これらもシ

11

システム・バス110に結合されている。これらの入出力ポートは、例えば、ブロードキャスト・インタラクティブ・テレビジョン・コンポジット信号を受信し、テレビジョン・モニタおよびスピーカ用のビデオ信号とオーディオ信号を出力し、電話システム経由でリモート・コンピュータに接続し、および/または視聴者ロケーションに置かれたローカル・パーソナル・コンピュータに接続するためのものである。入出力アダプタをどのように設計し製造すると、これらのサービスが得られるか、また、これらのアダプタをどのようにシステム・バス110に接続するかは、コンピュータ・システム設計分野に精通したものであれば当然に理解されることである。

【0030】スマート・カード20はCPU202を内蔵し、このCPUは、システム・バス210を介して公知のようにRAM204、ROM206、EEPROM208および入出力ポート212に結合されている。セット・トップ・ボックス10側の入出力ポート112は、コネクタ30を介してスマート・カード20側の入出力ポート212に結合されている。

【0031】図2は一部がブロック図に、一部がデータフロー図になっているが、これは、図1に示すセット・トップ・ボックス10とスマート・カード20のオペレーションの理解を容易にするためである。図2に示すエレメントで、図1に示されているものには、同一の参照符号を付けてあり、以下で詳しく説明することは省略する。図2に示すラインは図示エレメント間のデータの流れを示すもので、それぞれの物理的接続を示したのではない。

【0032】図1を参照してオペレーションを説明すると、セット・トップ・ボックス10内のCPU102はRAM104、EEPROM108、および入出力ポート112などの入力ポートからデータを取り出し、そのデータを処理し、処理したデータをRAM104やEEPROM108にストアしておくことも、処理したデータを入出力ポート112などの出力ポートへ渡すこともできるが、これらはすべて、ROM106に格納されているプログラムの制御を受けて公知の方法で行われる。図2に示すように、EEPROM108は、システムに関する情報420を収めているシステム部分416と、ユーザに関する情報422を収めているユーザ部分418を含むように区画化されている。同様に、RAM104も、システムに関する情報を収めているシステム部分424と、ユーザに関する情報を収めているユーザ部分426を含むように区画化されている。

【0033】ブロードキャストまたは電話リンク（図示せず）を介してセット・トップ・ボックス10に渡されるインタラクティブ・プログラムはトークンの形体になっており、これは、公知のように、セット・トップ・ボックス10内のインタプリタによって解釈される。インタラクティブ・プログラムは1つまたは2つ以上のコー

12

ド・モジュールと、場合によっては、1つまたは2つ以上のデータ・モジュールとからなっている。図4に示すように、コード・モジュールはRAM104内のコード・セクション402に格納され、データ・モジュールはデータ・セクション404に格納されている。ROM106に格納されているインタプリタ406はセット・トップ・ボックス10内のCPU102によって実行され、それぞれがRAM104のコード・セクション402とデータ・セクション404に置かれているコード・モジュールとデータ・モジュールを解釈するように動作する。インタラクティブ・プログラムは、インタプリタ406の制御の下でデータをデータ部分404から読み取り、そのデータを処理し、変更したデータをデータ部分404に書き戻すことができる。また、インタプリタ406は、同じくROM106に格納されているハードウェア・ドライバ408へのプログラム・コールを通して、公知のようにセット・トップ・ボックス10内のハードウェアともやりとりする。

【0034】ライブラリ・ルーチン群410は、インタプリタ406からプログラム・コールを通してアクセス可能であるが、共通に必要なファンクション (functions) 用に用意されたものである。スマート・カード入出力ドライバ408A、EEPROM108、およびRAM104、424および426のシステム部分とユーザ部分がアクセスできるのは、ライブラリ・ルーチン410への正しいコールを通してだけである。ライブラリ・ルーチン410はユーザの許可を要求し、それを受け取ってからセンシティブ情報を上記ソースのいずれかからインタラクティブ・システムへ返却するように事前にプログラムしておくことが可能である。基本的には、ライブラリ・ルーチン410は、それぞれEEPROM108およびRAM104、424、426のシステム部分とユーザ部分に格納されているデータのソフトウェア・ゲートキーパ（門番）の働きをする。ライブラリ・ルーチン410にゲートキーパ機能があるために、EEPROM108およびRAM104、424、426のシステム部分とユーザ部分は、それぞれRAM104、402、404のコード部分とデータ部分よりも相対的に安全度の高い記憶媒体になっている。さらに、EEPROM108はRAM104から物理的に切り離されているので、EEPROM108はRAM104よりも相対的に安全度の高い記憶媒体になっている。

【0035】図1に戻って説明すると、スマート・カード20内のCPU202は、入出力ポート212経由でセット・トップ・ボックス10からデータを受け取り、その情報を処理し、入出力ポート212経由で情報をセット・トップ・ボックス10へ返却するようにプログラムされており、これらはすべてROM204に格納されたプログラムの制御の下で行われる。ROM204に事前プログラムされているオペレーションだけが、スマー

ト・カード20内のCPU202によって実行される。例えば、セット・トップ・ボックス10の購入時に、購入者をユニークに識別すると共に、暗号解読（および暗号）キーの働きをするマスタ・キーは、入力ポート212からスマート・カード20に入力される。マスタ・キーは非常にセンシティブな情報である。スマート・カード20内のCPU202はマスタ・キーをEEPROM208にストアするようにプログラムされている。図2に示すように、スマート・カード20内のEEPROM208はシステム部分とユーザ部分に分割することが可能である。CPU202はマスタ・キー302をEEPROM208のシステム部分にストアする。

【0036】図1に戻って説明すると、暗号化されたデータがブロードキャストからセット・トップ・ボックス10によって受信され、暗号解読する必要があるときは、その暗号化データは入出力ポート212からスマート・カード20に渡される。スマート・カード20内のCPU202はEEPROM208に以前にストアされていたマスタ・キー302を使用して、暗号化データを暗号解読し、プレーンテキスト (plaintext) を入出力ポート212経由でセット・トップ・ボックス10へ返却する。同様に、CPU202は入出力ポート212から受け取ったプレーンテキストを暗号化し、暗号化されたデータを入出力ポート212経由でセット・トップ・ボックス10へ送り返す。CPU202はマスタ・キー302をセット・トップ・ボックス10へ戻すようにプログラムされていないので、セット・トップ・ボックス10で実行されているプログラムがマスタ・キー302を変更したり、取得したりすること、場合によっては、マスタ・キーを盗むことは不可能である。CPU202はスマート・カード20に格納されたデータのハードウェア・ゲートキーパ（門番）の働きをするので、セット・トップ・ボックス10側のEEPROM108またはRAM104よりも相対的に安全度が高く、非常に安全度の高い記憶媒体になっている。

【0037】上述したように、セット・トップ・ボックス10側のEEPROM108とRAM104はスマート・カード20側のCPU202のようなハードウェア・ゲートキーパによって保護されていない。その代わりに、EEPROM108とRAM104の保護はライブラリ・ルーチン410を通してソフトウェアで実現されている。しかし、EEPROM108とRAM104はソフトウェアによって保護されるので、その保護が偶然にしろ、意図的にしろ、他のソフトウェアによって違反される可能性が常にある。インタラクティブ・プログラムは、保護ソフトウェアをだますことによってEEPROM108またはRAM104へアクセスできる潜在性をもっている。例えば、正しくないデータがリロケーション（再配置）プロセス期間にプログラム・ローダ（図示せず）に渡されたり、あるいはプログラム・スタック

（図示せず）がプログラム実行中に意図的にオーバフローしたりするおそれがある。要するに、ソフトウェア保護が他のプログラムによって破られるおそれがある。

【0038】上述したように、最も安全度が高い記憶媒体はスマート・カード20であり、次に安全度が高いのはセット・トップ・ボックス10内のEEPROM108であり、次がRAM104のシステム部分412とユーザ部分414であり、最も安全度が低いのがRAM104のコード部分402とデータ部分404である。センシティブ情報のセキュリティ（安全保護）を最大にするには、この情報は、マスタ・キー302と同じように、スマート・カード20側のEEPROM208に置いておくべきである。しかし、スマート・カード20側のEEPROM208のサイズは限られているので、センシティブ情報をストアできるスペースはわずかしかなかった場合がある（マスタ・キー302は別として）。あるいは、スペースがまったく残っていない場合も起こり得る。セット・トップ・ボックス10側のEEPROM108のサイズも、同様に限られているので、センシティブ情報をストアできるスペースはわずかしかなかった場合もある。従って、ユーザのセンシティブ情報の大部分はRAM104にストアせざるを得ないことになるが、これは最も安全度の低い記憶媒体である。

【0039】スマート・カード20にストアできる以上のセンシティブ情報量を安全にストアするために、まず、センシティブ情報は上述したように、スマート・カード20にストアされたマスタ・キー302を使用してスマート・カード20側のCPU202によって暗号化される（例えば、データ暗号化規格 (Data Encryption Standard - DES) を使用して）。そのあと、暗号化されたセンシティブ情報は相対的に安全度の低いEEPROM108にストアすることも、RAM104のシステム部分412またはデータ部分414にストアすることも可能である。さらに、センシティブ情報の変更を防止するために、センシティブ情報全体にわたる暗号チェックサムも、例えば、市販されているハッシュ関数 MD5などの、一方向暗号ハッシュ関数 (one-way cryptographic hash function) を使用して計算され、情報に付加される。（MD5はCounterpane Systems 社、730 Fair Oaks Ave., Oak Park Illinois, 60302からディスクットに入って提供されている。）チェックサムはプレーンテキストのセンシティブ情報全体にわたって生成することも、暗号化されたセンシティブ情報全体にわたって生成することも、その両方で生成することも可能である。好適実施例では、チェックサムは暗号化されたセンシティブ情報全体にわたって生成されている。チェックサムは、CPU202またはCPU102を使用してソフトウェアで生成することも、バス構造に結合された専用ハードウェア・ハッシュ関数エレメント（図示せず）で生

成することも可能である。暗号化されたセンシティブ情報をアクセスできないプログラムは、スマート・カード 20 に格納されているマスタ・キー 302 がなければ、その情報を暗号解読して、読み取ることはできない。さらに、暗号化された情報を変更しようとしても、その試みは、以前に計算されて情報に付加された暗号チェックサムと、新たに取出したセンシティブ情報全体にわたって同じように計算された暗号チェックサムとの不一致によって検出される。

【0040】スマート・カード 20 はデータを暗号化する前に、ユーザの許可を要求する。これは、パーソナル識別番号 (PIN) をユーザに要求することにより行われる。なお、この PIN は好ましくは 4~6 文字の ID になっている。PIN はセット・トップ・ボックス 10 のベンダに選択させ、あとでユーザが変更することができる。ユーザが与えた PIN が現在格納されている PIN に一致していれば、データは暗号解読される。正しくない PIN があらかじめ決めた回数 (例えば、4 回) 続けて入力されると、ユーザ以外のだれかがセット・トップ・ボックス 10 に侵入しようとしているものとみなされるので、マスタ・キー 302 は使用禁止にされる。

【0041】図 2 に示すように、セキュリティを最大にするために、PIN 304 はスマート・カード 20 にストアされる。PIN 304 はわずか 4~6 文字であり、4~6 バイトにストアできるため、スマート・カード 20 側の EEPROM 208 には PIN 304 をストアするだけの空きスペースを残すことができる。スマート・カード 20 側の CPU 202 が PIN 304 をリリースしないようにプログラムされていれば、PIN 304 をより安全に格納しておくことができる。視聴者が正しい PIN 304 を与えたときだけ、スマート・カード 20 は、要求側プログラムのためにセンシティブ・データを暗号解読する。これにより、センシティブ・データのリリースは安全な状態で視聴者の制御下に置かれることになる。

【0042】二次暗号キー、クレジットカード番号などのように、電源障害が起こったときユーザが残しておきたいと思っているセンシティブ情報は、セット・トップ・ボックス 10 側の EEPROM 108 にストアされる。この情報はスマート・カード 20 に入っているマスタ・カード 302 を使用して暗号化される。暗号化されたセンシティブ・システム情報 420 はセット・トップ・ボックス 10 側の EEPROM 108 のシステム部分 416 にストアされ、暗号化されたセンシティブ・ユーザ情報 422 は EEPROM 108 のユーザ部分 418 にストアされる。暗号化されたセンシティブ・システム情報 420 またはユーザ情報 422 をアクセスしようとする不正プログラムはその暗号解読をスマート・カード 20 に要求しなければならないので、ユーザから正しい PIN を受け取らない限り、スマート・カード 20 はそ

の要求を拒否することになる。PIN をランダムに送ってスマート・カードに侵入しようすると、その試みが数回失敗したあとでマスタ・キー 302 は使用禁止にされる。

【0043】しかし、上述したように、EEPROM 108 も、センシティブ情報をストアできるスペースが限られている。従って、電源障害が起こったとき残しておきたい重要な情報だけが上記と同じように EEPROM 108 にストアされる。図 3 に示すように、相対的に安定度の低い RAM 104 には、もっと多くのセンシティブ情報をストアすることが可能である。この情報は暗号化され、暗号チェックサムは EEPROM 108 のシステム部分 416 に暗号化形式で格納されている二次暗号キーの 1 つを使用して付加される。暗号化されたセンシティブ・システム情報は RAM 104 のシステム部分 412 にストアされ、暗号化されたセンシティブ・ユーザ情報は RAM 104 のユーザ部分 414 にストアされる。RAM 104 のメモリ要求量は低下しているのも、もっと多くのセンシティブ情報を RAM 104 にストアすることができる。

【0044】この情報をアクセスするには、EEPROM 108 に格納されている、暗号化された二次暗号キーがまず暗号解読されなければならない。二次暗号キー自体も、スマート・カード 20 に格納されたマスタ・キー 302 を使用して以前に暗号化されているので、上述したように、この二次暗号キーがスマート・カード 20 によって暗号解読されるのは、これも上述したように、ユーザの許可を受け取ったあとだけである。暗号解読された二次キーがスマート・カード 20 から返されれば、RAM 104 にストアされたセンシティブ情報はこのキーを使用して暗号解読することができる。RAM 104 には、EEPROM 108 やスマート・カード 20 よりも多くのスペースが残っているのも、より多くのセンシティブ情報を RAM 104 にストアすることができる。その場合でも、この情報が無断アクセスから保護されているのは、その暗号解読のためには、スマート・カード 20 にストアされているマスタ・キーが最終的に必要になるためである。

【0045】図 4 に示すように、上述した手法はユーザ PIN をストアするだけのスペースがスマート・カード 20 に残っていない場合でも使用することができる。図 4 に示すように、マスタ・キー 302 だけがスマート・カード 20 にストアされている。PIN は暗号化され、暗号チェックサムはマスタ・キー 302 を使用して付加され、暗号化された PIN 304' はシステム情報 420 の一部として、セット・トップ・ボックス 10 側の EEPROM 108 のシステム部分 416 にストアされる。図 4 に示す実施例では、スマート・カード 20 はデータを暗号解読するように要求されると、暗号化された PIN 304' を EEPROM 108 から取り出し、そ

17

れを暗号解読して、その暗号チェックサムを以前にストアされた暗号チェックサムと比較する。暗号チェックサムが同一であれば、PINがユーザに要求され、暗号解読されたPINと比較される。これらが同一であれば、要求されたデータが暗号解読される。上述したように、正しくないPIN番号が続けて入力されると、マスターキー302のオペレーションは禁止される。また、上述したように、センシティブ情報は暗号化してRAM104にストアすることができる。

【0046】セット・トップ・ボックス10の特定実施例によれば、独自の公用・私用キーのペアが生成され、ストアされ、管理されるようになっている。このような実施例では、セット・トップ・ボックス、つまり、BOXは、シグネチャ（署名）に対してRivest、ShamirおよびAdleman 公用キー・アルゴリズムRSAを採用するように構成されている。RSAアルゴリズムでは、2つの基数 p と q （ただし、 $p < q$ ）、およびサイズBOX PUBLIC MODULUS SIZE/2 とサイズBOX EXPONENT SIZE の任意の指数“ e ”の各々を生成し、ストアすることが要件になっている。これらの3つの値 p 、 q 、 e からは、RSA暗号化を行うための、他のすべてのパラメータを求めるときに必要な一切の情報が得られる。しかし、公用キーの各シグネチャまたは照会ごとに他のパラメータを求めるために計算負担（penalty）が伴うことは望ましくないもので、システムはパラメータを一度だけ（または少なくともBOXがリセットされるたびに）生成し、それぞれの値をストアしておいて、反復的に使用するようになっている。これらの値はBOX内の安全保護された不揮発性メモリにストアしておくべきであるが、この種の記憶容量は上述したように限られている。従って、これらの値はRAMに安全にストアされて、データの保全性と機密性が保証されるようにしている。

【0047】上述したことは次のように行われる。値 p と q は生成されるか、あるいは与えられて、BOXモジュラス(modulus) “ n ” が $n = p \times q$ に従ってBOX CPU102またはスマート・カードCPU202によって計算される。BOX EXPONENT値“ e ”は選択されるか、あるいはあらかじめ決められて、EEPROM108などの不揮発性ストレージ(storage)にストアされる。値 n と e は、アクセスを容易にするためにブレンテキストとしてRAM104にストアされる。値 n と e は公用キーとなり、従って、公用キー・システムでは公衆に知られるので、機密に保持しておく必要はない。値 p と q は、シード・ワード(seed word) が128ビットに初期設定されている疑似乱数ジェネレータを使用して生成される。この疑似乱数ジェネレータは、少なくともその一部にMD5などのハッシュ関数を含めることができ、CPUによってソフトウェアで実行させることが可能である。

【0048】その他の値（私用キーを得るための）はC

18

PUによって次のように計算される。

【0049】1. $dp = e^{-1} \pmod{(p-1)}$

2. $dq = e^{-1} \pmod{(q-1)}$

3. $p^{-1} \pmod{q}$

4. $p^{0p \text{ prime}}$ および $q^{0q \text{ prime}}$ (Montgomery縮小(reduction)のために使用される単一単位値)

値1~4はランダムに選択したDESキー K を使用して暗号化され、暗号化されたデータはRAM104にストアされる。ハッシュ（例えば、MD5）は、少なくともRAM内のこのデータについて行われ、チェックサム C が生成される。値 p 、 q 、 e 、 K および C は安全保護された不揮発性ストレージ208にストアされる。チェックサムは安全保護されたストレージにストアされたデータ全体にわたって生成され、データに付加される。このようにして、データが相対的に安全度の低いRAM104に置かれていても、その保全性と機密性が保持されることになる。

【0050】RAM内のデータが利用される前に、不揮発性メモリ内の安全保護データ全体にわたってチェックサムがとられ、付加されているチェックサムと突合わせ検査される。これらのチェックサムが同一であれば、チェックサム C が安全保護された不揮発性ストレージ208からアクセスされ、保全性チェックがRAMデータについて行われる。つまり、RAMデータでハッシュが行われて、別のチェックサム C^* が生成され、これは対応するチェックサム C と比較される。この比較または以前の比較が失敗したときは、データは壊れているものとみなされ、安全保護データとRAM記憶データはデフォルト値にセットされる。これらのチェックサムが同一であれば、キー K がアクセスされ、RAMデータが暗号解読され、利用されることになる。つまり、アイテム1~4がアクセスされ、私用キー暗号化で使用する。DES暗号化はスマート・カード20によって行われるが、これは好ましい方法である。別の方法として、BOXに別の暗号化/暗号解読ハードウェアを含めることも可能であり、その場合は、このハードウェアがアクセスされてRAM内の値のDES暗号化と暗号解読が行われることになる。

【0051】上述した手法を使用すると、相対的に安全度の高い記憶媒体に格納された暗号キーを使用して情報を暗号化し、暗号化されたセンシティブ情報を相対的に安全度の低い記憶媒体にストアしておくことができるので、相対的に大量のセンシティブ情報を安全な状態で相対的に安全度の低い記憶媒体にストアしておくことができる。

【0052】図5はマルチメディアまたはインタラクティブ・テレビジョン・レシーバをブロック図で示している。信号はアンテナ80によって検出され、チューナ検出器81に入力され、そこで受信信号の特定の周波数バンドが抽出され、ベースバンド多重化パケット信号が得

られる。周波数バンドは、システム・コントローラ89 (以下、IRDコントローラという) を通してユーザによって選択されるが、その方法は従来と同じである。公称的には、ブロードキャスト信号は、例えば、Reed-Solomon順方向エラー訂正(forward error correcting - FEC)符号化を使用して、すでにエラー符号化されている。従って、ベースバンド信号はFECデコーダ82に10 入力される。FECデコーダ82は受信ビデオを同期化し、定期的に、あるいは例えば、メモリ・コントローラ87から要求があったとき、パケットを出力する。どちらの場合も、パケット・フレーム化または同期信号はFEC回路から得られ、それぞれのパケット情報がFEC82から送出された回数を示している。

【0053】単一プログラム信号からのパケットだけがレシーバによって処理される。この例では、多重化パケット・ストリームからどのパケットが選択されるかは、ユーザが知らないものと想定している。この情報はプログラム・ガイドに入っているが、このガイド自体もプログラムであり、それぞれのサービス・チャンネルID、つまり、SCIDを通してプログラム信号コンポーネントを相互に関係づけるデータからなっている。プログラム・ガイドは各プログラム別にリストしたもので、そこには、それぞれのプログラムのオーディオ、ビデオ、およびデータ・コンポーネントのSCIDが含まれている。プログラム・ガイドには、一定のSCIDが割り当てられている。レシーバに電源が入ったとき、IRDコントローラ89はプログラム・ガイドに関連するSCIDをSCID検出器84にロードするようにプログラムされている。なお、SCID検出器は整合フィルタのバンクにすることができる。プログラム・ガイドSCIDが検出されると、メモリ・コントローラ87は対応するパケット・ペイロードをメモリ88内のあらかじめ決めたロケーションに送るように条件づけられており、これはIRDコントローラによって使用される。

【0054】IRDコントローラは、インタフェース90を通してユーザからプログラミング・コマンドが送られてくるのを待っている。なお、インタフェースはキーボードが図示されているが、これは従来のリモート・コントロールにすることも、レシーバ・フロント・パネル・スイッチにすることも可能である。ユーザはチャンネル4 (アナログTVシステムで通常言われている用語) から送られてきたプログラムを見ることを要求したとする。IRDコントローラ89は、チャンネル4のプログラム・コンポーネントのそれぞれのSCID別にメモリ88にロードされていたプログラム・ガイド・リストをスキャンし、これらのSCIDをSCID検出器84にロードするようにプログラムされている。

【0055】要求されたプログラムのオーディオ、ビデオまたはデータ・プログラム・コンポーネントの受信パケットは、最終的には、それぞれのオーディオ・プロセ

ッサ93、ビデオ・プロセッサ92、または補助データ信号プロセッサ91 (94) へ送らなければならない。データは相対的に一定のレートで受信されるが、信号プロセッサは、公称的には、データがバーストで入力されることを要求している (ただし、例えば、圧縮復元 (伸張) のそれぞれのタイプによる)。図5に例示するシステムでは、まず、それぞれのパケットはメモリ88内のあらかじめ決めたメモリ・ロケーションへ送られる。そのあと、それぞれのプロセッサ91~94はコンポーネント・パケットをメモリ88に要求する。コンポーネントをメモリ経由で送るようにすると、ある程度の望ましい信号データ・レートのバッファリングやスロットリングを行うことができる。

【0056】オーディオ、ビデオおよびデータ・パケットはそれぞれのあらかじめ決めたメモリ・ロケーションにロードされ、各プロセッサがコンポーネント・データを容易にアクセスできるようにしている。それぞれのコンポーネント・パケットのペイロードは、対応するSCIDと、SCID検出器から出された制御信号に応じて該当のメモリ・エリアにロードされる。この関連付けはメモリ・コントローラ87にハードワイヤ (hardwired) することができるが、プログラマブルにすることも可能である。

【0057】それぞれの信号パケットはFEC82から信号デスクランブラ (signal descrambler) 86を経由してメモリ・コントローラ87に結合されている。それぞれの信号パケットはヘッダとペイロードを含んでいる。信号ペイロードだけがスクランブルされ、パケット・ヘッダは未変更のままデスクランブラによってパスされる。パケットがデスクランブルされるかどうかはパケット・ヘッダのフラグによって決まり、パケットがどのようにデスクランブルされるかはパケット・ヘッダの二番目のフラグによって決まる。このパケット・デスクランプリングは、上述したアプリケーション・モジュール・セキュリティ処理からほぼ独立している。

【0058】インタラクティブ・システムには、マルチメディア信号のデータ部分と共に動作できる複数のデバイスを含めることが可能である。例えば、図5において、AUX1プロセッサとAUX2プロセッサはどちらも、信号のデータ部分にตอบสนองして動作するようになっている。AUX1プロセッサは、送信株式市場データを検出し、そのデータを送信インタラクティブ・アプリケーションで操作するように構成されたパーソナル・コンピュータPCにすることができる。AUX2は、送信インタラクティブ・コマーシャルと関連づけてインタラクティブな衝動買いができるように構成されたテレビジョン・システムにすることができる。なお、インタラクティブは、図5のシステムと相互接続された電話モデム (図示せず) を使用すると容易化される。さらに、IRDコントローラ89は、特にシステム保守を目的に、送信ア

10

20

30

40

50

21

アプリケーションを処理し、実行するようにプログラムすることが可能である。

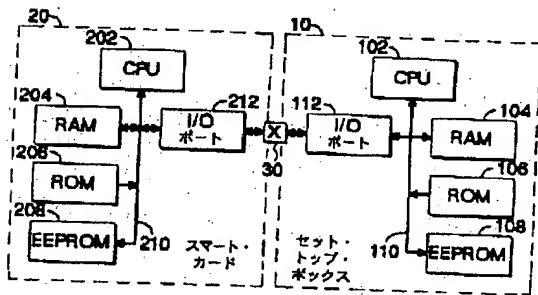
【0059】この例において上述したセンシティブ情報のストアはシステム・コントローラ89によって行われるが、この例では、システム・コントローラはROM、安全保護された不揮発性ストレージおよびスマート・カードを含んでいるものと想定している。RAM104はメモリ88のあらかじめ決めたブロックで構成することが可能である。ハードウェア・ドライバ408はメモリ・コントローラ87に含まれている。この例では、図5

【図面の簡単な説明】

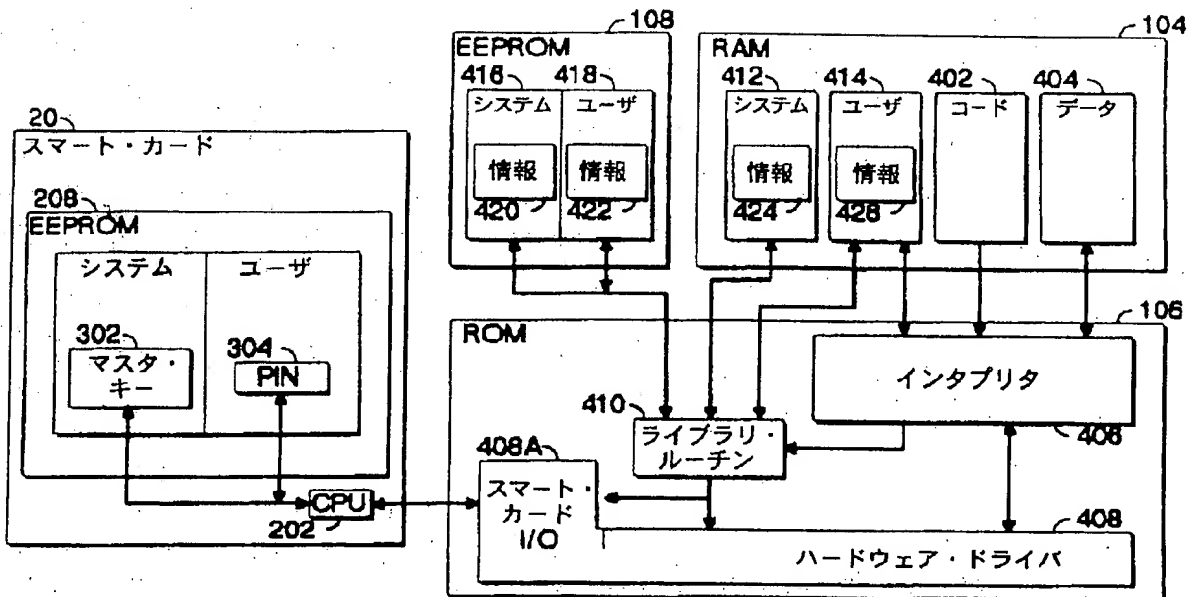
【図1】本発明を取り入れているインタラクティブ・テレビジョン・デコーダを示すブロック図である。

【図2】本発明を取り入れているセット・トップ・ボッ

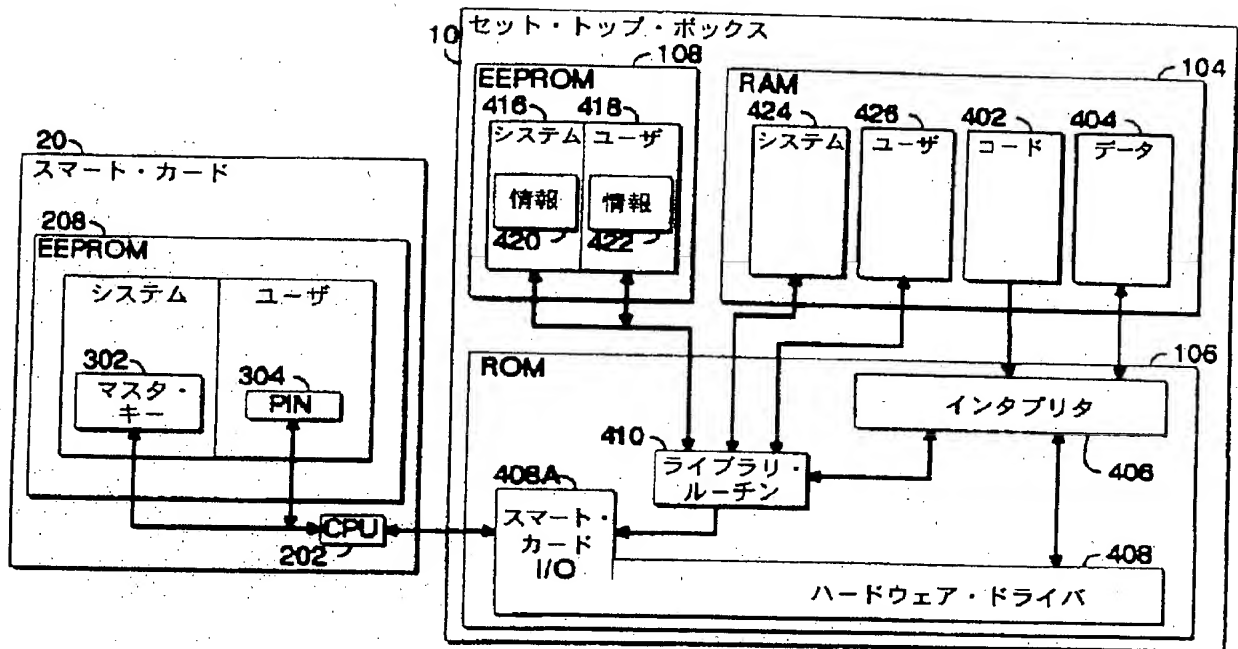
【図1】



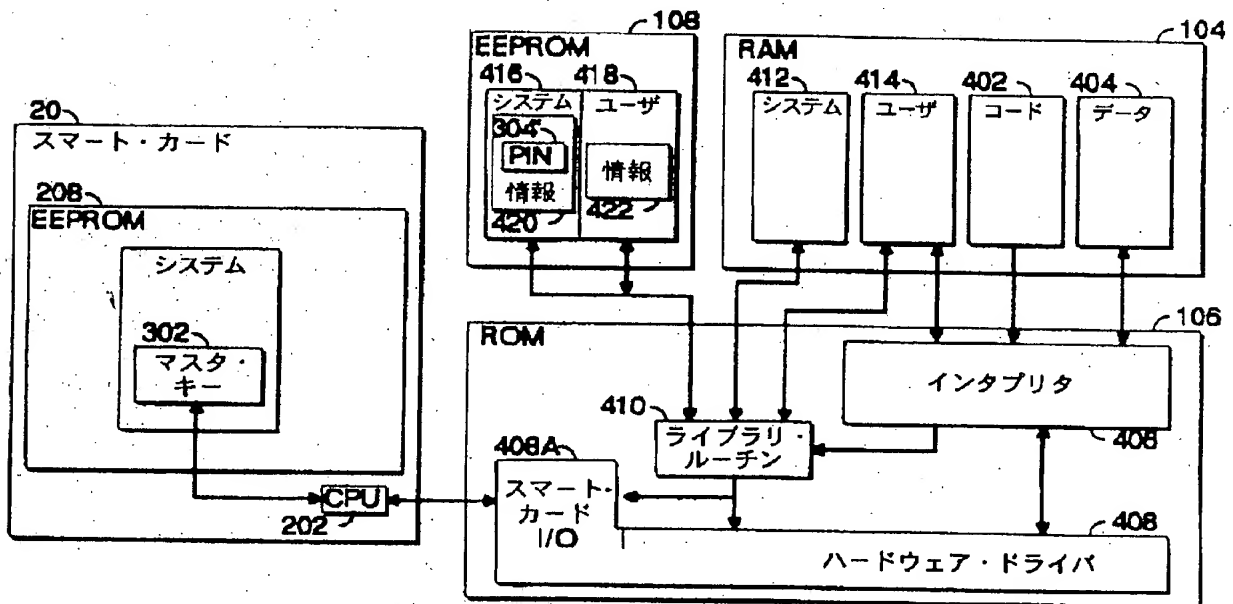
【図3】



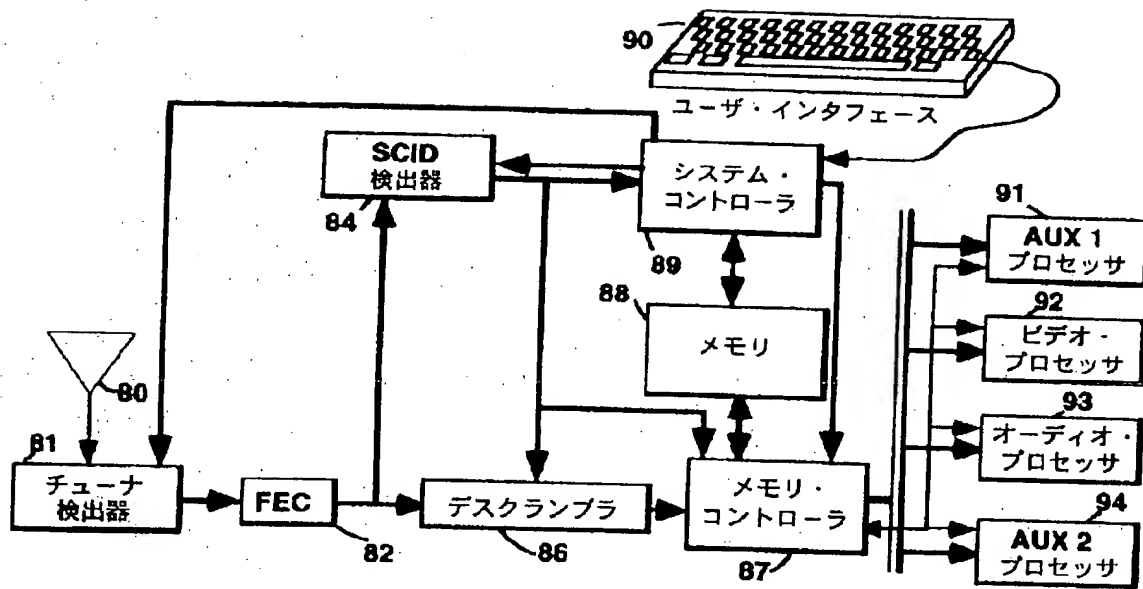
【図2】



【図4】



【図5】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☒ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.